Virus Protection And Safe Computing

Common questions about computer viruses and how to live with them

The answers apply mainly to the Microsoft Windows operating system.

For information about Macintosh and Linux antivirus programs see:
http://antivirus.about.com/ or

http://www.info.apple.com (Search on Security)

First- The Essentials
1. Install an antivirus suite and keep it up to date. This is more comprehensive than just an antivirus program and normally includes online support.

2. Update your operating system and Internet applications with the latest "patches". In the case of Windows, use Windows Update to install Critical Updates from the desktop Startmenu or at:
http://windowsupdate.microsoft.com

3. Update Microsoft browsers via Windows Update :
http://windowsupdate.microsoft.com
or from the Microsoft Download Centre
http://www.microsoft.com/downloads/search.aspx?displaylang=en

4. Install a Firewall normally included, especially if you have a cable or ADSL connection (See here)

5. If you have the choice, do not login to your Operating System as Administrator, but as a User. See Networks and Passwords

6. Be aware, keep informed, practice Safe Computing by reading Defensive Computing or take advice from one of the following:
http://www.microsoft.com/security/protect/

http://www.f-secure.com/virus-info/tips.shtml and

http://www.info.apple.com/usen/security/index.html for Apple users

7. And subscribe to email newsletters for virus information. See here for more

What is a Virus (or a Worm or a Trojan)?

All of these can be called Malware, or Malicious software.

A virus is a computer program or code that replicates itself and infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself.

A worm is a program that copies itself from one disk to another by email or other transport mechanism. Worms infect computers, but do not infect files. They can simply be identified and then deleted. However, they often make registry or startup file changes so that they are executed on boot-up. They are now very sophisticated, can avoid detection by antivirus programs and even disable them (and firewalls), so that you may have no protection whatsoever. It is probable that a lot of spam is sent out from such infected computers, unknown to the owner of the machine.

A trojan is a program that neither replicates nor copies itself; it may arrive in an email, in a program, or by simply viewing a web page (if your browser has an unpatched vulnerability). It can be commanded to do tasks such as sending information away from your computer, or it may open a "back door" which allows a remote computer to control your machine.

Spyware is sometimes planted in your computer without your knowledge or permission when you install a new program or while you are connected to the Internet.

All must be regarded as harmful, though some viruses and worms are not. See https://www.symantec.com/security_response/glossary/ for definitions.

Why should you be concerned about viruses?

Because you are likely to be infected at some time, especially if you take no precautions.

Although your ISP may have a virus scanner for email, some viruses may slip through. You can also be infected from other sources such as some Internet sites (Web surfing), removable media (floppy disks, CD-ROMS etc), and Internet messaging (Windows Messaging, IRC etc) or file-sharing (via Internet or internal network).
Infection with a virus may result in great inconvenience, the possible loss of some of your data and programs, revelation of your private information (including passwords and credit card numbers), or even destruction of your

system.

You may also spread the infection to many other users via addresses stored on your computer, or in files you share with others. Your computer could be taken over and made a base for attacks on others. Therefore, it is in everybody's interest for you to be informed about how viruses spread, and ways to avoid and control them. And it is important to recognise a Hoax for what it is, so as not to be panicked into unnecessary action.

How will I know if I have a virus?

You may be alerted by other persons who believe you have sent them a virus. This may not be true, because Melb PC and other ISPs scan mail for viruses, and many viruses use false "from" addresses which are randomly selected or generated. The message bearing the virus most likely came from a computer on which your address is recorded, but you should check your system nevertheless.

Or you may be alerted by your antivirus software, if installed. Exactly what message did your anti-virus software give you? Write this down before you click the "OK" button that dismisses the warning.

You may be alarmed! because your computer is behaving abnormally - cant open some programs, strange things happening, it locks up, or wont start. But do not assume a virus is responsible for any computer problem that may be readily and simply fixed. And note that even if some odd system behaviour is due to a virus, the "three R" solution (re-partition, reformat and reinstall) is seldom necessary or appropriate.

You may also get a False Alarm in the form of a Joke or a Hoax. False alarms can be more time-consuming and wasteful than actual virus detection incidents. Hoaxes come in email messages or attachments, are often in bold or capital letters, offer exciting rewards, or warn you to do something to prevent some catastrophe. They may be harmless, but can cause a lot of trouble if you follow their instructions. Do not forward any such warning message to all your contacts without verification. A good website to check if it is a Hoax is: http://www.symantec.com/avcenter/hoax.html

How could I have got a virus when I have antivirus protection installed?

Your AntiVirus program may not be up-to-date, or more likely your operating system and browser have not had the latest "patches" installed. This is particularly important when upgrading to or reinstalling a new operating

system, after which you are vulnerable until you have installed the patches to bring it up to date.
You may have taken the precaution of installing AntiVirus software, but lapsed in keeping it and your operating system updated. To be effective, antivirus software should have been updated within the last week at least, best within the last 24 hours. Or you may have been unlucky enough to acquire one of the latest new viruses, for which a signature update has not yet been prepared (it takes at least a few hours for new virus threats to be countered, and for your software company to offer a "fix"). Download and install the latest update when it becomes available, then do a full scan of your system.

What should I do if I have a virus?

Don't panic!
Help is available if you ask for it. Always contact your Antivirus software vendor first, or look for advice on their webpage if you can.

Contact MelbPC Internet Help by telephoning the First Aid (Help) line (10 am to 3pm) or the MelbPC office to avoid using your computer. But read on, to help yourself.

- **Avoid using your computer**, especially to go online, until the virus is "cleaned". Most viruses are transmitted by email, but by simply connecting to the Internet you can be sending copies of the virus out of your computer. The virus usually has its own means of sending mail out even when you are not accessing your email account. So, only connect to the Net if you have to, for example, to get help, or to obtain an Update or Patch for your operating system, or to update your AntiVirus Suite (subsequently referred to here as AVS, see below). And make sure your Firewall is active if you do need to connect, especially for updates to Windows XP. Then disconnect till your computer is cleaned.

- **If you have an Anti-Virus Suite (AVS)** - Check that it is up to date. This means it has been updated within the last week at least, best within the last 24 hours. If it is not up to date (and it probably is not if you have acquired a virus), then do so at once. Then do a full scan of all your hard disks. This means that the scan includes boot sectors, memory, and files of all types, including those in subfolders. Most AVS's are set to do this by default, after a Typical or Standard installation, but you should check the configuration if you feel capable. Try the toolbar of the program, possibly under Options.

It is unwise to scan for viruses with an out-of-date AVS because the program must open the files to scan them. If the AVS cannot recognise or destroy the virus(es) it may release or activate some that have until that time been dormant. If you have taken the precaution of installing anti-virus software, but have had a temporary lapse in its maintenance, it will be easier to recover from a virus infection.

Likewise, if you were unlucky enough to have acquired the very latest virus for which a signature update has not yet been prepared, it will be simpler and quicker to download and install the latest update when it becomes available than to start from scratch. All AVS's, and particularly updates, must be obtained from a reliable source.

- **If you do not have an AVS** - Ask for help from MelbPC (see above), or buy a commercial AVS, online or on CD-ROM, or download a free AVS from http://www.free-av.com/ or

  http://www.avg.com/au-en/homepage

  Note that a free program may be less useful than one you pay for, e.g. you may not get telephone support, or updates may be less frequent. And you may sooner or later be required to pay for it. The AVS you obtain may be a few months old. It is unwise to scan for viruses with an out-of-date AVS because the program must open the files to scan them. If the AVS cannot recognise or destroy the virus(es) it may release or activate some that have until that time been dormant. It must be updated to be effective. This must be done online before you (next)

  Do a full scan on all your hard disks (see 2 above). The scan should report that the virus has been cleaned, deleted, quarantined or neutralised. It may also tell you if some elements could not be removed, or that the scan was incomplete (e.g. unable to scan .zip, .cab,or .dat files).

- **If your computer will not start**, and you have a Rescue Diskette created when you installed your AVS, this might be the time to use it, but you will need to know what to do. If you are not sure, try contacting your AVS support line first. If you do not have a Rescue disk, you may be able to recover with a bootable Startup disk, plus appropriate advice. Occasionally a virus will need to be removed in Windows Safe

Mode, or by booting into DOS (and use an AV Program for DOS), because it can escape detection and removal when Windows is started in the usual way.

- **Transmission of the virus** In most cases, the virus/worm selects addresses in your address book and message folders, and even anywhere on your hard disks, to which it send copies of itself by email. It is not practicable to hide or delete these addresses, and most viruses/worms make up false ones anyway! So the best you can do is to avoid going online, or to minimise the length of time you stay connected to the Net until the virus has been cleaned.

- **AVS's cannot eradicate all viruses completely.** While the Internet Help (iHelp) team will give whatever help they can, expert help may be required from the AVS vendor by telephone, or from their website. Some viruses, by their nature, cannot be "cleaned". They may have created new files which remain on your system (residual files), and these may need to be removed manually (including editing the Windows Registry), or require a Removal Tool. They may also have renamed, altered or deleted some files. This may require reinstallation from original or backup copies of your software. Occasionally a virus will need to be removed in Windows Safe Mode, or by booting into DOS (and use an AV Program for DOS), because it can escape detection and removal when Windows is started in the usual way.

- **Change your passwords**. Some types of malware steal your passwords and other information, sending it away to a remote site. So it is advisable to change passwords and to review all security settings after recovering from a virus attack. It is good practice to change your passwords periodically.

What can I do to protect my computer from viruses?

The most important things are

to install good AntiVirus software (see What anti-virus programs are recommended? for a list), and to keep it constantly updated,

to update your operating system and browser, which for almost everyone is Windows and Internet Explorer (see Internet Explorer Updates and Windows Updates, below), and

to install, activate, and properly configure a Firewall

Operating System and Internet Explorer Updates -

Some email programs are particularly targeted by virus writers, e.g. Outlook and Windows Live Mail. These are vulnerable because of their association with Internet Explorer. When you look at an HTML message in the preview pane or open message window you're actually looking at a browser window. So any vulnerability of Internet Explorer is 'inherited' by the email program. because of Internet Explorer's close integration with Windows. Internet Explorer can be "patched", but if you don't install the patches, simply changing to Thunderbird, Opera, Eudora, or The Bat as your email client will not protect you if you retain the vulnerable copies of Internet Explorer on your computer. Most users do not try to uninstall Internet Explorer completely (though it is possible), so the recommended updates and patches should be installed, otherwise the susceptibility remains. Currently it is recommended to upgrade to Internet Explorer for later versions of the Windows operating system. You can have it installed and still use a different browser or email client if preferred.

The IE installation from the Web should be Typical or Full, not Minimal or Custom, or preferably, install it from a MelbPC Monthly CD-ROM which is quicker and more reliable.

All versions of Internet Explorer require updates or patches. Updates for early versions are now hard to find!

Get updates for later versions via Windows Update (Go to Windows Update from Internet Explorer | Tools menu and follow the prompts), which can be configured to update automatically (see below), or accessed via these links: http://windowsupdate.microsoft.com,

You are advised to install "Critical" Updates for Internet Explorer and for your version of Windows.

What antivirus programs are recommended?

This is a matter of personal preference, as all the well-known programs are effective. A Web search will lead to information and download sites. Here is a list which is not comprehensive, and is in alphabetical order and not necessarily by recommendation :

- **Avast** – https://www.avast.com/en-au/index
- **AVG** – (owned by Avast) http://www.avg.com/au-en/homepage
- **Avira** - https://www.avira.com/
- **AVG** – (owned by Avast) http://www.avg.com/au-en/homepage
- **CA Anti-Virus** - https://www.ca.com/us.html
- **F-Secure/F-Prot** - https://www.f-securestore.com.au/
- **Kaspersky Anti-Virus 2009** - https://www.kaspersky.com.au/
- **NOD32** - https://www.eset.com/us/home/antivirus/
- **Norton Anti-Virus** - https://au.norton.com/
- **Sophos** - http://www.sophos.com/
- **Trend Micro (PC-Cillin)** - http://www.antivirus.com/
- **Vet** (owned by Computer Associates- see CA Anti-Virus above)

Can I get a free antivirus program?

Yes, but note that a free program may be less useful than one you pay for, e.g. you may not get telephone support, or updates may be less frequent. Or you may sooner or later be required to pay for it. Note that after installing the program it is necessary to update it regularly.

Avast! Personal Edition available from https://www.avast.com/en-au/index

AVG Personal Edition, from http://www.avg.com/au-en/homepage

Avira Personal Edition is available from https://www.avira.com/

Will I be completely protected if I install an antivirus program?

No, because no anti-virus checker can be said to be 100% effective, even if it is frequently updated. There is a constant battle between virus writers and virus eradicators, and variants may appear when the code is altered slightly. New viruses are appearing all the time, and may infect some computers before a "fix" is written for them. And an AVS will not help if your operating system is not "patched" up to date.

It would be wise to adopt "defensive computing" practices, see Defensive

Computing
Even if your ISP (e.g., MelbPC) provides virus scanning on your Internet connection, a virus may occasionally slip through, so it is important to have your own virus protection. There are other sources of infection also.

Are there any software programs that are immune from virus attack?

The answer to this has to be "No", but virus creators tend to concentrate their efforts on the programs that are most widely used, so that the virus spreads easily and has maximum effect-usually damaging! It is true that some are less likely to be attacked, or less vulnerable. But see How can I protect my computer from viruses? for an explanation of major weaknesses, and Defensive Computing (below).

Are there any software programs that are immune from virus attack?

The answer to this has to be "No", but virus creators tend to concentrate their efforts on the programs that are most widely used, so that the virus spreads easily and has maximum effect-usually damaging! It is true that some are less likely to be attacked, or less vulnerable. But see How can I protect my computer from viruses? for an explanation of major weaknesses, and Defensive Computing (below).

Defensive Computing (Other precautions you can take)

- **Never open attachments to emails (even from an apparently trusted source, because the "From" address can be faked, called "phishing")** or never open without first scanning them with an up-to-date Anti-Virus Suite (AVS). Your anti-virus software may be set to do it by default, but you can do it manually to be sure. You may choose to open only those attachments which you have asked someone to send to you (and you should scan them too). Regard all unsolicited mail and forwarded messages (even if forwarded from someone you know) as suspicious. Beware of persuasive messages with strange headings, or invitations that promise rewards or excitement. For image files, open the viewing application (e.g., IrfanView) first and open the pictures in it, instead of double-clicking on the attachment. Don't trust the icons or file extensions on attachments; they may be deliberately falsified to mislead you into opening a file which seems harmless. Try to get all attached documents sent to you in Rich Text Format (*.rtf), or do not enable macros in Word.

- **Show all file extensions** Configure Windows to always show file extensions. From Windows Explorer | Tools | Folder Options, uncheck "Hide file extensions for known file types". Then it will not be possible for an EXE or VBS file to masquerade as a TXT or JPG file. And never open attachments with extensions VBS, SHS, or PIF, which are almost never used in normal attachments. Also, do not open attachments with double file extensions, like NUDE.JPG.EXE or NAME.DOC.PIF.

  Microsoft NEVER DISPLAYS .shs, .pif, and .lnk file extensions, whether you have hide file extensions on or off. Therefore, as further protection for MelbPC members, all attached files with extensions as above (plus .scr for good measure) passing through the MelbPC virus checker will be renamed with an underscore replacing the first letter of the extension. With the underscore, they are no longer executable under Windows unless the missing letter is replaced (at your own risk!).

  Other Executable files (e.g., .exe, .htm,.html) may also have a double extension (.bad) added . You may try renaming them as .txt and opening them in a text editor like Notepad, or you can restore the executable extension as above. The attachments are unchanged otherwise.

- **Disabling the Preview pane** In Outlook and Outlook Express, Auto preview and Preview respectively can allow activation of a virus in a message being viewed in the pane (see explanation under IE Updates "What can I do...?" above). In other words, if the message is highlighted, (one message in the list always is), it will open in the Preview Pane without being clicked. This is a useful feature that many do not want to disable.

  It need not be disabled if the appropriate updates have been installed, and your Anti-Virus Program is kept up to date.
  To disable the Preview pane:

  - In Outlook Express, from View|Layout|remove tick from Show preview pane.

  - In Outlook, from View|Define views|Tick messages and not messages with autopreview.

- **Previewing your mail on the mail server** You can avoid having to download your mail before you read it (and this is also one way of disposing of Spam mail) by using programs such as MailWasher which

also allows you to set bounce back criteria "for lists where unsubscribe proves difficult". But don't use it to bounce SPAM; this is quite ineffective as many "from" addresses are fictitious, and you will merely increase traffic on the Internet (and specifically on our Internet feed), with messages either returning to the wrong address, or being marked undeliverable, and returned. MailWasher works with all email programs unless they are Web based such as Hotmail, Yahoo and AOL. MailWasher can be found as a free download at: http://www.mailwasher.net/

MailWasher Pro with increased functionality is available at: https://www.firetrust.com/products/mailwasher-pro/download

- **Or you can use Office365:**

  1. Or via the External (http://office365.com) then Webmail Access).

  Then enter your username and password and "login". Here, you can see the size of your mailbox, read, send, and delete messages, but you may not be able to download them to your computer.

- **Review Security Settings** In Internet Explorer, these should be set at "Internet", in Tools | Internet Options | Security, and Custom Level should be "Medium". In Outlook Express, from Tools | Options | Security set the level to "Restricted Sites Zone", and tick "Warn me if other applications try to send mail as me". Do not tick "Do not allow attachments to be saved or opened that could potentially be a virus" unless you DO NOT have an up-to-date antivirus program, because if you do, some attachments which do not contain viruses (but are regarded by Microsoft as potentially harmful), may be barred.
  This is a view of Security Settings opened in Internet Explorer via "Tools"

- **Other sources of infection** Be Aware that other viruses can reach you via infected files in floppy disks or CD-ROMs, in files downloaded from the Internet (including newsgroups), or exchanged via IRC, ICQ, etc. (for example, see: http://www.irchelp.org/irchelp/security/trojan.html), and by simply browsing some Web pages or clicking on innocent-looking messages. This may include reading messages in Hotmail, Yahoo Mail, and AOL, though email scanning is now very effective. So an up-to-date Operating System and AVS with Resident protection are

essential.

As a general rule, when in doubt never click "OK" or "Close", rather "kill" the dialogue box with the "X" in the top right-hand corner.

If you have a Floppy Disk drive it is also recommended to set the startup sequence in the BIOS to C:A:, CD-ROM, C:A:, or just C:(or HDD) to prevent inadvertent booting from a floppy disk infected with a boot virus left in the drive. In the event that you need to boot from A:, you will need to reset the BIOS by entering Setup during the bootup process.

- **Resident Protection should be enabled in your AntiVirus Suite**
  This is AntiVirus protection which is activated when the computer is started, and then remains "on watch" in the background. It may also be called by other names, e.g. Real-Time Monitoring. Most Resident programs will watch for executable file types, detecting them when they are downloaded or copied, or when a file is opened. Some programs, but not all, scan email messages also (usually only incoming messages, by default). But many viruses are programmed to disable AVSs.

  Any AVS installed on your computer is useless if it is inactivated. Sometimes the AVS may be disabled to prevent it interfering with another program, e.g. while running Windows Defrag, or it may be turned off while installing a new software program, and you may forget to turn it on again. Check that Resident Protection is enabled, usually by right-clicking the AVS icon in the "Tray" at the lower right hand corner of your computer screen, and selecting "Status" or a similar option, or by opening the program and checking (usually) Options.

  You can be test your system for virus infection with free scanning programs at:
  "Housecall" http://housecall.trendmicro.com/au
  or at
  http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ie&venid=sym

  NOTE: these URLs MUST be in ONE LINE if copied or typed - or use the main site address and then navigate from there.

Networks and Passwords

If you are connected to a network and have file-sharing enabled, important files should be password-protected. Viruses spread very easily and quickly on networks. Passwords should be jealously guarded, and changed periodically, particularly after a virus attack. If your operating system has Administrator or Root privileges, login as a User instead of as Administrator, Superuser or Root. This will protect most of your files from being tampered with

Firewalls
Another line of defence is a firewall. These are normally included with a AVS and have become more necessary, even essential, as malware becomes more sophisticated. A firewall is strongly recommended if you are connected to your ISP by broadband (cable or ADSL) which, unlike Dialup connections, is "always on". Windows has a limited inbuilt firewall . It may not be enabled by default. To see if it is enabled go to Control Panel>Network Connections>Properties>Advanced and make sure the tick is in place under "Internet Connection Firewall", or see http://www.thundercloud.net/infoave/ for full illustrated instructions.

ZoneAlarm (http://www.zonelabs.com) is one in common use, but it is important to understand its actions and behaviour.
Kerio Personal Firewall (http://www.kerio.com) is another.

A firewall will block access to your computer from the Internet, and can also prevent information being sent away without your knowledge, depending on the instructions you give it. For either Resident protection or a firewall to be effective and trouble-free, each must be properly configured. Read the instructions carefully.

Firewalls should be tested to see if they are effective. Go to "Shields Up" at http://www.grc.com/

Only use one Firewall as more may fight each other and slow down the computer.

Subscribe to a (Free) AntiVirus Newsletter

Stay informed! This will get you virus alerts, details of new viruses and hoaxes, tips, and much useful information. This includes descriptions of how to recognise suspicious mail headers and message wording. From any of the major AntiVirus program vendors, e.g.,
https://www.sophos.com/about-us.aspx or

http://www.antivirus.com/

Visits to their websites will also yield much useful information, e.g., http://www.ca.com,

https://www.symantec.com/security_response/,

http://www.europe.f-secure.com/v-descs/ or

http://antivirus.about.com/

Virus alerts and detailed information on new viruses can be found by clicking the "Latest Virus Advisory" link at: http://www.auscert.org.au/

Revised LW May 2017